IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>*Plaintiff*<br><br>v.<br><br>STEPHEN WAYNE CORMACK<br>*Defendant* | Criminal No. ELH-19-0450 |

**MEMORANDUM OPINION**

In this case, the Court must resolve, *inter alia*, the legality of a warrantless, after-hours entry into the office of the defendant, Stephen Wayne Cormack, and the search of his work computer. At the time, the defendant was an employee of the Maryland Department of General Services ("DGS"), an agency of the State of Maryland. The results of the computer search led to the issuance of several search warrants that were allegedly tainted by the initial search. The various searches culminated in child pornography charges against defendant.

In particular, Cormack was indicted on September 19, 2019, and charged with one count of possession of child pornography, in violation of 18 U.S.C. § 2252(A)(a)(5)(B). ECF 1. In a Superseding Indictment filed on April 19, 2021 (ECF 40), two charges were added for receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), (b)(1), and 2256.

The defendant filed a "Consolidated Motion To Suppress Tangible And Derivative Evidence." ECF 32 (the "Motion"). He asserts violations of his rights under the Fourth Amendment to the Constitution in connection with a total of four searches, of which three occurred pursuant to a warrant.

In the Motion, the defense focuses primarily on the warrantless entry into defendant's locked office, identified as "Office C," and the warrantless search of defendant's work computer,

conducted on March 28, 2019, by TFC Frank Donald of the Maryland State Police ("MSP"); John Evans, then the Chief Information Security Officer for the Maryland Department of Information Technology ("DoIT"); and Detective Sergeant Warren Smith of the Maryland Capitol Police, which is the security arm of DGS. The search was limited to defendant's work computer; no search was made as to defendant's desk or personal belongings.

In addition, Mr. Cormack challenges the execution of two search warrants on May 2, 2019. Both warrants were issued by a Maryland State judge. One was for defendant's residence on Lyndale Avenue in Baltimore County, and the other was again for Office C.

Further, the defendant challenges a search warrant issued by United States Magistrate Judge J. Mark Coulson on May 15, 2019, upon application of Special Agent Augustus Aquino of Homeland Security Investigations ("HSI"). The warrant authorized the search, *inter alia*, of various devices and electronic equipment seized during the earlier searches. These included defendant's desktop computer, his laptop computer, thumb drives, media, and SD cards seized from his home, his vehicle, and Office C. According to the government, the searches revealed over 3,800 images and over 300 videos of child pornography.

The government opposes the Motion. Its corrected opposition is at ECF 44, supported by several exhibits. No reply was filed.

The Court held a hearing on May 21, 2021. At the hearing, the government called four witnesses and introduced several exhibits.[1] The defense did not present any evidence.

For the reasons that follow, I shall deny the Motion.

[1] As of this writing, I do not have a transcript of the proceedings. Therefore, in recounting any testimony, I have relied on my notes.

## I. Factual Summary

Cormack was an employee of DGS, a Maryland State agency, from 1999 until his termination in 2019. Among other things, DGS is responsible for over six million square feet of State owned facilities and over four million square feet of leased space. *See* dgs.maryland.gov (last visited May 25, 2021). Its customers include the occupants of those facilities. *Id.*

The defendant worked at the State Office Building located at 301 West Preston Street in Baltimore, where he was assigned to Office C on the 14th floor. According to the testimony of Lauren Bucker-Duncan, an Assistant Secretary of DGS, defendant worked in the Office of Design and Construction, and was the archivist for blueprints with respect to State construction projects.[2] He also managed supplies and printing.

On August 28, 2000, defendant signed an "Acknowledgement Receipt" (ECF 44-1; Gov't. Ex. 1) acknowledging his receipt of the DGS Employee Handbook (the "Handbook", ECF 44-2; Gov't Ex. 2).[3] The Handbook contains several directives, including one titled "Acceptable Use Statement for Computing Resources" ("Directive"). *Id.* at 3.

Section I of the Directive provides that the "Purpose" of the "document" is to set forth the "acceptable use" of the "computing systems and equipment owned and operated" by DGS, to include "any computer, server, or network provided or supported" by DGS. *Id.* at 4. Further, Section I states: "The purpose of this acceptable use statement is to ensure that all DGS users . . . use the DGS computing systems and facilities in a[n] effective, efficient, ethical and *lawful manner*." *Id.* (Emphasis added).

[2] Ms. Buckler-Duncan was appointed by the Secretary of DGS. She is one of four assistant secretaries.

[3] For the convenience of the reader, and where possible, I shall cite to the exhibits by reference to the electronic record associated with the government's opposition as well as the exhibit numbers assigned at the hearing.

Section II of the Directive is titled "General Policy." *Id.* It provides that "DGS computing resources are to be used only for the purpose for which they are authorized . . . ." *Id.* Further, Section II informs employees that DGS "may monitor network traffic, e-mail transmissions, and internet activity." *Id.*

Paragraph 8 of Section II advises: "Electronic communication facilities (such as Email or Internet) are for authorized government use only." *Id.* at 5. It adds: "Fraudulent, harassing or obscene messages and/or materials shall not be sent from or stored on DGS systems." *Id.*

In Section III of the Directive, titled "Violations," it warns that failure to comply "will constitute a security violation" and may result, *inter alia*, in "criminal prosecution." *Id.*

The Secretary of DGS is appointed by the Governor. On August 4, 2016, Ellington Church, Jr., then the Secretary of DGS, circulated a Memorandum to all DGS personnel regarding inappropriate use of email and the Internet. ECF 44-3; Gov't Ex. 3 ("Memorandum"). The Secretary instructed DGS personnel as follows: "Electronic communications are to be used only for authorized government business." *Id.* In addition, he warned that DGS "has a zero tolerance policy for the inappropriate use of State email and internet resources." *Id.* Further, the Secretary stated that "obscene" materials may not be "created with, sent from, to, or stored on DGS systems." *Id.* And, he stated, *id.*: "Accessing sexually explicit . . . websites is also a violation of the Department's eMail and Internet policy." The Memorandum concluded: "The Department will not tolerate the inappropriate use of this electronic medium and violators will continue to be dealt with severely."

As noted, the defendant was assigned to Office C on the 14th floor of the State Office Building in Baltimore. His name was posted on a sign outside the door to Office C. The office contained a desk as well as a State-owned computer and related equipment. *Id.* It also contained

office supplies for use by other DGS employees, as well as numerous filing cabinets and drawers for architectural blueprints, drawings, and other documents managed by defendant and used by other DGS employees. Some of the drawers are used to store drawings as large as two feet by three feet. *See* Gov't Ex. 15A (Transcript of interview of co-worker) at 11.

During working hours, the door to Office C was typically open. Ms. Buckler-Duncan testified that other DGS employees had access to Office C to retrieve supplies and documents. They did not require permission to enter Office C. Although defendant locked the door to Office C when he was not at work, he was not the only DGS employee with a key to that office. According to Ms. Bucker-Duncan, another DGS employee also had a key to Office C. Moreover, she stated that defendant and the other State employee who had a key to Office C were not permitted to be off from work on the same day. In other words, this assured the ability to access Office C, even if defendant was not at work.

The government presented a video of Office C. Gov't Ex. 4. It depicts defendant's desk in the room, along with a computer. The desk is rather small, without drawers. And, the room appears sizeble. It is filled with file cabinets, file drawers, and supplies. The evidence also included photos of stickers on the computer equipment, indicating that the computer equipment was the property of the State of Maryland.

Significantly, when a DGS employee attempts to log onto a work computer, a warning banner is displayed. ECF 44-5; Gov't Ex. 5. At the relevant time, the warning banner said: "Welcome to the Department of General Services Network." *Id.* It also stated, in part, *id.*: "WARNING: This computer system is for authorized users only. Unauthorized access to this computer is a violation of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. *Use of this computer, including e-mail, is monitored. The Office of the Attorney General has the*

*right to inspect, without notice to the user, any work created, including all e-mail messages sent or received, on this computer*." (Emphasis added).

The word "Warning" appeared in capital letters. In order to log in, the user had to click "OK" with respect to the warning. In other words, in order to access the computer, the employee had to agree to the terms.

In January 2019, a DGS co-worker was in Office C and was disturbed by an image he saw on defendant's work computer. The co-worker notified Ms. Buckler-Duncan that he believed he saw the defendant viewing an image that the co-worker thought was child pornography. He described the photograph in some detail.

In turn, Ms. Bucker-Duncan reported the matter to Tonya Sturdivant, the Director of Human Resources for DGS. The matter was subsequently reported to the Maryland Capitol Police, the security component of DGS, and to the Office of the Maryland Attorney General.

Defendant's co-worker was interviewed on February 5, 2019, by Detective Smith and TFC Donald. The interview was recorded (Gov't Ex. 15) and excerpts of the interview were played at the hearing.[4] A transcript was also introduced, without objection. Gov't Ex. 15A ("Transcript" or "Tr.").

The co-worker is an architect. Tr. at 10. He stated that he has known the defendant for about 20 years. Tr. at 4, 5. He disclosed that defendant had a prior child pornography conviction. Tr. at 6, 10.

During the interview, the co-worker described the image he saw on defendant's work computer. It was an image of a male child, approximately 8 years of age, clad only in

[4] The identity of the co-worker was redacted in the submissions. But, he certainly is not anonymous. His identity was known to his supervisor at DGS and to the individuals who interviewed him and recorded his statement. The parties did not indicate whether his identity has since been made known to the defendant.

underwear, and the child appeared to be "scared" and "terrified." Tr. at 1, 2. According to the co-worker, as soon as he entered Office C, the defendant "shut the picture . . . ." Tr. at 3.

According to the co-worker, the defendant always has his personal laptop with him at work. Tr. at 7. And, he stated that the defendant "does tend to migrate from his State computer" to his "personal laptop." *Id.* Moreover, whenever the co-worker would enter Office C, the personal laptop "gets closed immediately." *Id.* He also indicated that "there's a backup drive [to the computer] that goes home with [the defendant] every night." *Id.*; *see also id.* at 8.

In addition, the co-worker recalled a suspicious incident several years earlier involving defendant and a website with the title "Young Japanese Boys." Tr. at 12. The co-worker regretted that he did not say anything at that time, but he "thought that was a fluke . . . ." Tr. at 10.

The co-worker provided a drawing of the floor plan of the 14th Floor. Gov't Ex. 14. It showed the location of Office C.

After that interview, TFC Donald of the Maryland State Police obtained State records that reflected that in 1996 defendant was convicted of second degree sexual assault. The conviction related to the sexual abuse of several male minors while the defendant was employed as a counselor at a recreation center in Parkville, Maryland.

John Evans, then the Chief Information Security Officer for the Maryland Department of Information Technology, was informed of the co-worker's report concerning Mr. Cormack. The DoIT is generally responsible for information technology policy for the State. *See* msa.maryland.gov (last accessed May 25, 2021). It develops, maintains, and enforces policies, procedures, and standards, including security requirements, for most Maryland State agencies.

*Id.* Evans attempted to investigate the defendant's computer usage remotely. But, he testified that he was unable to obtain the defendant's internet search history.

At about 11:13 p.m. on March 28, 2019, Evans signed a form that authorized the Maryland State Police to enter Office C and search the defendant's work computer. *See* ECF 44-6; Gov't Ex. 6. Nevertheless, he testified that he did not have authority to authorize entry into the office itself. But, Evans consented to a search of the computer in Office C.

Detective Sergeant Smith explained that the Maryland Capitol Police is responsible for security for State buildings. And, as part of his duties, he had a key to Office C as well as the authority to enter the office. He stated that he authorized the entry into Office C on the evening of March 28, 2019.

During a forensic preview of the external hard drive at defendant's work station, investigators observed an image of a male minor, estimated to be 14 or 15 years old, engaged in masturbation. The image was located in the recycle bin of the external hard drive for the computer. Investigators imaged the external hard drive, cloned the internal hard drive of the computer and replaced it, and took the hard drives. The computer had cables attached to it that would allow the user to attach an additional external hard drive. But, an additional hard drive was not attached at that time.

According to the government, subsequent review of the hard drives revealed that on March 8, 2018, there were 12 searches from the work computer for child pornography. *See* ECF 44 at 7.[5] On September 9, 2018, there were searches from the work computer on the video streaming website Youtube.com for "boys skinny dipping." *Id.* And, files of prepubescent boys

[5] The government did not introduce evidence concerning the review of the hard drives. The information recited here is found in the government's opposition to the Motion.

were stored in the "My Documents" folder on the work computer. *Id.* In addition, the internet browser history reflected information materials about child sex abuse and child pornography. *Id.*

TFC Donald subsequently obtained warrants from Judge Wayne Brooks, a Maryland judge, to search Office C (ECF 44-7; Gov't Ex. 7) and the defendant's residence on Lyndale Avenue in Baltimore County. ECF 44-8; Gov't Ex. 8. The warrants were executed on May 2, 2019.[6]

At his residence, the defendant was advised of his *Miranda* rights, signed a waiver, and agreed to an interview. ECF 44 at 8. No motion was filed to suppress the statement. Moreover, no evidence was presented at the hearing regarding the content of the statement or its voluntariness.[7]

Electronic equipment and storage media were seized from defendant's residence, from his vehicle, and from Office C. Among other things, law enforcement seized an Acer laptop, several SD cards, two digital cameras, and other storage media.

---

[6] The warrant for the search of defendant's home did not include defendant's vehicle. Nevertheless, the vehicle was also searched on May 2, 2019.

In their written submissions, the parties did not address the search of the defendant's vehicle on May 2, 2019. Upon inquiry by the Court at the hearing on May 21, 2021, defense counsel stated that the defendant does not challenge the vehicle search.

[7] According to the government's opposition, the defendant stated that the briefcase he ordinarily takes to work was located in his car, parked in front of the house. ECF 44 at 8. It contained two external hard drives, and one of the hard drives contained a backup of the files for work. *Id.* The other hard drive, according to the defendant, contained family photos and personal documents, not pornography. *Id.* The defendant claimed he did not use his work computer to review child pornography. But, he used Goggle and, if child pornography popped up, he would look at it. *Id.* Cormack also stated that he had a personal laptop in his office, either on his desk or in a cabinet. *Id.* He described it as an Acer laptop computer, and said he usually does not bring it home. *Id.* He explained that he has it at work because he has a color printer and he uses the computer to print family photos. *Id.*

On May 15, 2019, HSI obtained a federal search warrant signed by Magistrate Judge Coulson to examine items seized during the searches, including the Acer laptop computer and SD cards seized from Office C. *See* ECF 44-9; Gov't Ex. 9. According to the government, forensic examination of the Acer laptop computer, its internal hard drive, and a SansDisk SD card revealed approximately 3,800 images and over 300 videos of child pornography. ECF 44 at 8-9.

Additional facts are included, *infra*.

## II. Discussion

### A. The Fourth Amendment Generally

The Fourth Amendment to the Constitution protects against unreasonable searches and seizures. *Utah v. Strieff*, ____ U.S. ____, 136 S. Ct. 2056, 2060 (2016); *United States v. Mendenhall*, 446 U.S. 544, 551 (1980). It guarantees, *inter alia*, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Of relevance here, the Fourth Amendment "applies as well when the Government acts in its capacity as an employer." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 756 (2010); *see also Treasury Employees v. Von Raab*, 489 U.S. 656, 665 (1989).

However, the Fourth Amendment "does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991); *see Whren v. United States*, 517 U.S. 806, 809-10 (1996); *Illinois v. Rodriguez*, 497 U.S. 177, 183 (1990); *United States v. Sharpe*, 470 U.S. 675, 682 (1985); *Mendenhall*, 446 U.S. at 551. Thus, "the ultimate touchstone of the Fourth Amendment is reasonableness." *Fernandez v. California*, 571 U.S. 292, 298 (2014) (internal quotation marks omitted); *see also Kentucky v.*

*King*, 563 U.S. 452, 459 (2011); *United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018); *United States v. Sowards*, 690 F.3d 583, 588 (4th Cir. 2012).

Under *Katz v. United States*, 389 U.S. 347, 351 (1967), a search occurs within the ambit of the Fourth Amendment when a law enforcement officer invades a person's "reasonable expectation of privacy." This is a concept that embraces "a twofold requirement[:] first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring). Conversely, "[w]hen there is no reasonable expectation of privacy, the Fourth Amendment is not implicated." *United States v. Davis*, 690 F.3d 226, 241 (4th Cir. 2012), *cert. denied*, 571 U.S. 829 (2013).

The "reasonable expectation of privacy" test was formulated by Justice Harlan in his "famous" concurrence in *Katz*. *See Payne v. Taslimi*, ___ F.3d ___, 2021 WL 2149364, at *4 (4th Cir. May 27, 2021) (recognizing that the reasonable expectation of privacy language "emanates from Justice Harlan's famous concurrence" in *Katz*). The Supreme Court has long recognized that "later cases have applied the analysis of Justice Harlan's concurrence" in *Katz*. *United States v. Jones*, 565 U.S. 400, 406 (2012); *see, e.g.*, *Bond v. United States*, 529 U.S. 334 (2000). Nevertheless, "Fourth Amendment rights do not rise or fall with the *Katz* formulation." *Jones*, 565 U.S. at 406. Rather, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Jones*, 565 U.S. at 409 (emphasis in original).

"[T]o demonstrate a legitimate expectation of privacy," the defendant "must have a subjective expectation of privacy." *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010). But, that subjective expectation of privacy must also be one that is "objectively reasonable," *i.e.*,

"it must be an expectation that society is willing to recognize as reasonable." *United States v. Bullard*, 645 F.3d 237, 242 (4th Cir. 2011) (internal quotation marks omitted); *see also United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (stating that a government agent's search is unreasonable when it infringes on "an expectation of privacy that society is prepared to consider reasonable."); *United Sates v. Castellanos*, 716 F.3d 828, 832 (4th Cir. 2013).

The reasonable person standard is an objective one, and "its proper application is a question of law." *United States v. Weaver*, 282 F.3d 302, 309 (4th Cir. 2002); *see United States v. Jones*, 678 F.3d 293, 299 (4th Cir. 2012). The defendant has the burden to demonstrate a legitimate expectation of privacy in the area subject to search. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980); *Castellanos*, 716 F.3d at 832.

As the Fourth Circuit said in *Lyles*, 910 F.3d at 795, "Reasonableness has many dimensions. One must be proportionality between the gravity of the offense and the intrusiveness of the search." The Court also said, *id.* at 796: "The magnitude of the intrusion relative to the seriousness of any offense 'is of central relevance to determining reasonableness.'" (quoting *Maryland v. King*, 569 U.S. 435, 446 (2013)).

Here, the entry into defendant's office was made without a warrant. And, the computer was searched without a warrant. Assuming that the Fourth Amendment applies, a warrantless search, *i.e.*, one "conducted outside the judicial process," is per se unreasonable unless the search falls within a valid exception to the warrant requirement. *See Kentucky*, 563 U.S. at 459-60; *Minnesota v. Dickerson*, 508 U.S. 366, 374 (1993); *Katz*, 389 U.S. at 357. The government bears the burden of proving, by a preponderance of the evidence, that a valid exception applies. *See United States v. Gwinn*, 219 F.3d 316, 335 (4th Cir. 2000).

**B. Search of March 28, 2019**

As noted, during the evening of March 28, 2019, TFC Donald of the Maryland State Police, Detective Sergeant Smith of the Maryland Capitol Police, and Evans, then the Maryland Chief Security Officer for the Department of Information Technology, made a warrantless entry into Office C and conducted a warrantless search of defendant's State-issued computer. According to the government's opposition, employees of the MSP Digital Forensics Lab were also present. ECF 44 at 6. But, no evidence was presented as to the presence of such individuals.

As indicated, the search of the computer was authorized by John Evans, then the Chief Information Security Officer for DoIT. The form that he signed also authorized entry into the office itself. DoIT was at least partly responsible for the State-owned computer that was the subject of the search.

At the time, defendant's name was posted outside the door to the office, and the office was locked. Entry to the office was made by way of a key provided by Detective Smith. He stated that he had authority to enter the office, based on his duties with the Maryland Capitol Police.

The entry to the office and the search of the computer cannot be characterized as a search conducted solely by the defendant's employer, given the presence of TFC Donald of the MSP. However, the search itself was very narrow in scope. It was limited to the computer that belonged to the State.

In analyzing the legality of the computer search, I am mindful of the Supreme Court's admonition in the case of *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010), concerning emerging technologies. The *Quon* Court cautioned that it "must proceed with care when

considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer." *Id.* at 759. It pointed to the "[r]apid changes in the dynamics of communication and information transmission" as well as changes in "technology itself" and "what society accepts as proper behavior." *Id.* Moreover, it recognized the uncertainty with respect to "workplace norms, and the law's treatment of them." *Id.* In addition, it acknowledged the "pervasive" presence of electronic communications, which would seem to "strengthen the case for an expectation of privacy" as to electronic devices." *Id.* at 760. Conversely, it pointed to "the ubiquity of those devices," which might also shape reasonable expectations of employees. *Id.*

With regard to the entry into Office C, Justice Blackmun's dissent in *O'Connor v. Ortega*, 480 U.S. 709 (1987) (plurality opinion), also seems apt. Joined by Justices Brennan, Marshall, and Stevens, Justice Blackmun observed that "the reality of work in modern time" is that for many "the workplace has become another home. . . ." *Id.* at 739.

As I see it, there are three avenues of analysis as to the events of March 28, 2019. Regardless of the road traveled, I reach the same result: the entry into Office C and the search of the computer were lawful.

**1. Expectation of Privacy**

As a threshold matter, I first consider whether the Fourth Amendment is even implicated with regard to the events of March 28, 2019.

The government maintains that the entry into Office C on March 28, 2019, and the investigation of the work computer, did not constitute a search subject to the Fourth Amendment. ECF 44 at 9. This is because, in the government's view, the defendant cannot demonstrate a

legitimate expectation of privacy "in these work facilities," and therefore the Fourth Amendment is not implicated. *Id.* at 10. I agree.

"Individuals do not lose Fourth Amendment rights merely because they work for the government . . . ." *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality opinion); *see also id.* at 731 (Scalia, J., concurring in judgment); *id.* at 737 (Blackmun, J., dissenting). But, a search implicates the Fourth Amendment only if the defendant had an actual or subjective expectation of privacy and the expectation is one that society is prepared to recognize as reasonable. *Kyllo*, 533 U.S. at 33; *Katz*, 389 U.S. at 361. Moreover, the defendant has the burden to prove a reasonable expectation of privacy. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980).

Whether an employee had a reasonable expectation of privacy turns on the particulars of the employment. *O'Connor*, 480 U.S. at 717-18. The question must be considered on a case-by-case basis. *Id.* at 717. Of import here, the expectation of privacy in "offices, desks, and file cabinets . . . may be reduced by virtue of actual office practice and procedures or by legitimate regulation." *Id.* Put another way, "operational realities" may impact an employee's privacy expectations. *Von Raab*, 489 U.S. at 671. Thus, "employer policies . . . will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." *Quon*, 560 U.S. at 760.

To begin, Office C was not used solely as defendant's office. Supplies, file cabinets, and file drawers were also stored in Office C. The file cabinets and drawers housed blueprints and other documents for State facilities. And, co-workers had complete access to the space while at work, whenever needed. It is also noteworthy that a fellow co-worker had a key to Office C. In the event that defendant was not at work, fellow workers retained access to Office C.

Moreover, DGS promulgated clear rules concerning appropriate computer usage. The information was disseminated via the Handbook and in a Memorandum issued by the Secretary of DGS in 2016 to DGS employees. Simply put, the agency did not permit use of the work computer to view child pornography, and defendant was clearly aware of the prohibition.

In addition, defendant was reminded about proper use of the computer each time he logged onto the computer, by way of a warning banner concerning computer usage. And, DGS warned employees that use of the computer was subject to monitoring.

In *O'Connor*, 480 U.S. 709, a physician employed by a state hospital in California alleged that hospital officials investigating workplace misconduct violated his Fourth Amendment rights by searching his office and seizing personal items from his desk and filing cabinet. He filed suit under 42 U.S.C. § 1983 and state law. Twenty-five years later, in *Quon*, the Supreme Court discussed *O'Connor* and explained that the *O'Connor* Court disagreed regarding "the proper analytical framework for Fourth Amendment claims against government employers." *Quon*, 560 U.S. at 756. But, a four-Justice plurality agreed on two steps to govern the correct analysis.

First, "a court must consider '[t]he operational realities of the workplace' in order to determine whether an employee's Fourth Amendment rights are implicated." *O'Connor*, 480 U.S. at 717. If an employee has a legitimate expectation of privacy, "an employer's intrusion on that expectation 'for non investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.'" *Quon*, 560 U.S. at 757 (quoting *O'Connor*, 480 U.S. at 725-26). The plurality noted that "'special needs, beyond the normal need for law enforcement, make the . . . probable-

cause requirement impracticable'" for government employers with respect to investigations of work-related misconduct. *O'Connor*, 480 U.S. at 725 (citation omitted).

As the *Quon* Court explained, Justice Scalia, who concurred in the judgment in *O'Connor*, "outlined a different approach." *Quon*, 560 U.S. at 757. Although Justice Scalia concluded that the Fourth Amendment protects the offices of government employees, "he would also have held 'that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment.'" *Quon*, 560 U.S. at 757 (quoting *O'Connor*, 480 U.S. at 732).

*Quon* was a § 1983 case involving the search of a police officer's text messages contained on a government device. The *Quon* Court cautioned that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer." *Quon*, 560 U.S. at 759. It noted that "the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Id.* The Court also pointed out that many employers "tolerate personal use" of the employer's equipment, and such reasonable use may be the norm. *Id.*

These admonitions seem as pertinent now as they were more than a decade ago, when *Quon* was decided. Yet, the admonitions have no bearing in the context of this case. This case does not involve emerging technology. It concerns use of a computer in a way that allegedly disregarded the employer's clear and unequivocal instructions as to its proper usage.

The case of *United States v. Simons*, 206 F.3d 392 (2000), supports the conclusion that defendant lacked a reasonable expectation of privacy with regard to the computer. In *Simons*,

the defendant, a government employee, was prosecuted for child pornography offenses after images of child pornography were discovered on his government-issued computer. *Id.* at 395. The agency that employed the defendant had instituted an internet usage policy for its employees that, among other things, "specifically prohibited" accessing "unlawful material," required employees to use the internet "for official government business only," and warned employees that the agency conducted extensive "electronic audits" of usage in order "'to support identification, termination, and prosecution of unauthorized activity.'" *Id.* (quoting policy). Pornographic images were discovered on the defendant's computer as a result of such auditing. *Id.* at 396. On appeal following his conviction, the defendant challenged the admission of the images on Fourth Amendment grounds.

The Fourth Circuit reiterated: "Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets. However, office practices, procedures, or regulations may reduce legitimate privacy expectations." *Id.* at 398 (internal citations omitted). And, "in light of the Internet policy" of the employer, the Fourth Circuit determined that the defendant "lacked a legitimate expectation of privacy in the files downloaded from the Internet" onto his employer-issued computer. *Id.* The Court reasoned that the policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private." *Id.*

The Fourth Circuit relied on *Simons* in the case of *United States v. Hamilton*, 701 F.3d 404, 408-09 (4th Cir. 2012). In *Hamilton*, the Court rejected a claim of marital privilege as to emails transmitted via a workplace computer system. It determined that the defendant had no reasonable expectation of privacy, in light of the employer's computer usage policy, which

advised that information received, accessed, or stored via the computer system was subject to inspection and monitoring.

In *Hamilton*, the Fourth Circuit recognized that "one may generally have a reasonable expectation of privacy in email." *Id.* at 408. But, the defendant's email account was provided by his employer, which had adopted a computer usage policy that "expressly provide[d] that users have 'no expectation of privacy in their use of the Computer System' and '[a]ll information created, sent[,] received, accessed, or stored in the . . . Computer System is subject to inspection and monitoring at any time.'" *Id.* (quoting policy). Moreover, the defendant "had to acknowledge the policy by pressing a key to proceed to the next step of the log-on process, every time he logged onto his work computer." *Id.* Therefore, the Court reasoned that the case was analogous to *Simons*, in which the Fourth Circuit had "held that a defendant did not have an 'objectively reasonable' belief in the privacy of files on an office computer after his employer's policy put him 'on notice' that 'it would be overseeing his Internet use.'" *Id.* at 408-09 (quoting *Simons*, 206 F.3d at 398).

The case of *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), also provides guidance. In that case, the computer use policy warned that system administrators could monitor usage and would turn over evidence of illegality to law enforcement. But, it did not explicitly warn users that law enforcement might be given direct access to the computer system. *Id.* at 1132-33. Nevertheless, the *Angevine* Court concluded that a university professor did not have a reasonable expectation of privacy. *Id.* at 1134-35. The court stated, *id.* at 1135: "[W]e have never held the Fourth Amendment protects employees who slip obscene computer data past network administrators in violation of a public employer's reasonable office policy." Therefore, it ruled that the defendant "could not have an objectively reasonable expectation of privacy," and

affirmed the district court's determination that "police did not need a search warrant to seize [Angevine's] University computer." *Id.* at 1132; *see also United States v. Bode*, ELH-12-158, 2013 WL 4501303, at * 19-20 (D. Md. Aug. 21, 2013) (concluding that defendant had no reasonable expectation of privacy in private chat messages when website warned user that messages could be disclosed).

Here, as indicated, DGS's computer use policy was set forth in the Handbook and defendant acknowledged receipt of the Handbook. And, the policy was reiterated and underscored in a Memorandum issued to DGS employees in 2016, again underscoring the parameters of improper use. Moreover, a warning banner was displayed on the computer every time it was accessed. In short, DGS employees were told repeatedly that the State owned the computer system and the data stored on it; the work computer was to be used for authorized work-related purposes only; and that usage is subject to monitoring. Therefore, defendant had no reasonable expectation of privacy as to the computer.

Nor could defendant have a reasonable expectation of privacy as to Office C. The office was not used solely by defendant. In fact, his co-workers had unfettered access to the room, as needed, for supplies, blueprints, and other documents. Nor was he the only employee with a key to the room. And, the video of the room confirms that Office C was a multi-purpose room. That defendant had his desk and a computer in Office C did not transform the room into one in which he had a reasonable expectation of privacy.

**2. Consent**

Alternatively, the government argues that the Fourth Amendment was not violated because the search was conducted with consent. In particular, the government argues that the defendant consented to inspection of the computer by clicking Ok every time he logged in to use

the computer. Moreover, the State, which owned the computer, also consented to the entry into Office C and to the search of the computer. According to the government, that law enforcement participated in the search did not vitiate the consent.

Of relevance here, "valid consent to seize and search items provides an exception to the usual warrant requirement." *United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973)), *cert. denied*, 550 U.S. 913 (2007); *see United States v. Ortiz*, 669 F.3d 439, 445 (4th Cir. 2011). And, consent can be provided by a person who holds either actual or apparent authority to consent. *Buckner*, 473 F.3d at 555; *see Rodriguez*, 497 U.S. at 188.

To be sure, consent is a "carefully drawn exception" to the warrant requirement. *Georgia v. Randolph*, 547 U.S. 103, 109 (2006) (citations and quotation marks omitted); *see United States v. Neely*, 564 F.3d 346, 349-50 (4th Cir. 2009) (per curiam). When the government justifies a warrantless search based on consent, it "bears the burden of establishing, by a preponderance of the evidence, that it obtained valid consent to search." *United States v. Toyer*, 414 F. App'x 584, 588 (4th Cir. 2011) (per curiam) (citing *Buckner*, 473 F.3d at 554); *see United States v. Robertson*, 736 F.3d 677, 680 (4th Cir. 2013); *United States v. Digiovanni*, 650 F.3d 498, 513-14 (4th Cir. 2011); *United States v. Block*, 590 F.2d 535, 539 (4th Cir. 1978). "This burden cannot be discharged by showing no more than acquiescence to a claim of lawful authority." *Bumper v. N. Carolina*, 391 U.S. 543, 548-49 (1968).

Here, State personnel possessed either common authority or apparent authority with respect to the Office and the computer. And, "the consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared." *United States v. Matlock*, 415 U.S. 164, 170 (1974); *Walker v.*

*Coffey*, 905 F.3d 138, 148-49 (3rd Cir. 2018). This includes consent to search a computer, even when it contains personal files of the employee and is password-protected. *United States v. Waddell*, 840 Fed. App'x 421, 431 (11th Cir. 2020).

The case of *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), is instructive. There, the Ninth Circuit considered the search of an employee's company computer based on a tip to federal agents from the internet service provider that the employee had accessed child pornography on the computer. *Id.* at 1185-86. The defendant, Ziegler, had a private office that he kept locked and the computer was password-protected. The company's IT administrator, who was authorized to monitor company computer usage, consented to a search of the computer. *Id.* at 1187.

In the view of the court, the search implicated the Fourth Amendment. *Id.* at 1189-90. Nevertheless, the Ninth Circuit upheld the warrantless search based on the valid consent provided by the company official. *Id.* at 1191-93. It recognized that a third party who possess "common authority over or other sufficient relationship to the premises or effects being inspected" may provide permission to a search by government agents. *Id.* at 1191 (cleaned up). Notably, the court concluded that the company could provide valid consent, despite the fact that the computer was password protected, because the company had the ability to access the computer and employees were on notice that the company could monitor activity on work computers. *Id.*

Here, Evans, then Maryland's Chief Information Security Officer, authorized the search of the computer. The form he signed also authorized the entry to Office C. And, Detective Smith also authorized entry into Office C. These two individuals either had common authority and/or apparent authority to consent to the entry.

**3.**

In *Quon*, discussed earlier, the Court considered the legality of the police department's review of an officer's text messages on a device provided to the police officer by his employer. The Court conducted its analysis based on the assumption of various propositions. These included that Quon had a reasonable expectation of privacy in the text messages on his work device provided to him by the employer; that the employer's review of transcripts of text messages constituted a search within the meaning of the Fourth Amendment; and principles applicable to search of a physical office applied to the "electronic sphere." *Id.* at 760.

As in *Quon*, I will assume, *arguendo*, that the Fourth Amendment applies to the warrantless search at issue. The outcome remains unchanged.

As indicated, a workplace search is not necessarily outside the ambit of the Fourth Amendment. In *O'Connor*, 480 U.S. at 725-26, the plurality recognized that, even if an employee has an expectation of privacy, a warrantless, work-related search is lawful if it is reasonable at its inception and reasonable in scope.

Relying on the *O'Connor* plurality, the *Quon* Court reiterated that a government employer's warrantless search is reasonable when conducted for a noninvestigatory, work-related purpose or for the investigation of work-related misconduct, so long as it is ""justified at its inception"' and reasonable in scope. *Quon*, 560 U.S. at 761 (citation omitted, cleaned up). And, the search does not necessarily fall outside the *O'Connor* framework, even if the purpose is to discover evidence of criminal activity. *See Simon*, 206 F.3d at 400; *United States v. Linder*, 12 CR 22-1, 2012 WL 3264924, at *11 (N.D. Ill. Aug. 9, 2012).

In this case, defendant's co-worker reported to his supervisor a belief that the defendant was engaged in improper use of the work computer. He also submitted to a recorded interview,

in which he provided a detailed statement of what he saw on the computer. He believed he saw child pornography. And, such use contravened clearly announced work policies.

For a search to be reasonable at its inception, there must be a reasonable basis to believe, *inter alia*, that the search will lead to evidence of work-related misconduct. *See Simons*, 206 F.3d at 400; *Gossmeyer v. McDonald*, 128 F.3d 481, 492 (7th Cir. 1997). This prong is readily met here, based on the information provided by defendant's co-worker.

The search related to the investigation of work-related conduct by defendant, notwithstanding that the same work-related conduct also led to the investigation of a violation of criminal law. Defendant has not provided the Court with any legal authority to support the proposition that the work-related investigation lost its character as an investigation of employee misconduct because it also involved the investigation of a crime. The search was justified at its inception because there were reasonable grounds to suspect a serious violation of work-related directives.

And, the scope of the search was entirely reasonable. It was limited solely to the State-owned computer and its components. No search was conducted of defendant's desk, the file cabinets, or any of defendant's personal effects.

Thus, I conclude that under *O'Connor* the entry into the office and the subsequent computer search were lawful.

**C. The Search Warrants**

The Warrant Clause provides that "no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and persons or things to be seized." A judicially authorized warrant is the cornerstone of the Fourth Amendment.

Two searches were conducted on May 2, 2019, each pursuant to a warrant issued by a State judge. One was for the defendant's home and the other was for Office C. Another search warrant was obtained in mid May 2019 from a federal magistrate judge for a search of electronic devices that were seized on May 2, 2019.

Defendant challenges all of the warrants as tainted fruit of the initial illegal search conducted on March 28, 2019. That argument fails, in light of my ruling that the initial search was lawful.

In addition, defendant argues that the affidavit in support of the search warrant application for defendant's home did not establish probable cause to believe that evidence of a crime would be found in defendant's home. ECF 32 at 5. In defendant's view, the warrant application lacked an adequate "nexus" between defendant's "suspected wrongdoing and his home." *Id.* According to Cormack, the "only connection" to his home "is the anonymous source," who claimed that defendant transported a backup drive every night from work to his home. *Id.* at 6.[8] Cormack insists, however, that there was no ground to conclude that the backup drive contained contraband. *Id.*

A constitutionally valid search warrant must describe with particularity the place to be searched and the items to be seized. *Davis*, 690 F.3d at 241. And, the warrant must be supported by probable cause to conclude that contraband, evidence, fruits or instrumentalities of a crime, or a fugitive, will be found at the location to be searched. F. R. Crim. P. 41(c); *Florida v. Harris*, 568 U.S. 237, 243 (2013); *United States v. Grubbs*, 547 U.S. 90, 96 (2006); *United States v. McNeal*, 818 F.3d 141, 150 (4th Cir. 2016); *United States v. DeQuasie*, 373 F.3d 509, 520 (4th Cir. 2004).

[8] As discussed, the co-worker was not anonymous.

To assess whether probable cause exists to issue a search warrant, a judicial officer must "make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983); *see Ornelas v. United States*, 517 U.S. 690, 696 (1996); *United States v. Ortiz*, 669 F.3d 439, 444 (4th Cir. 2011); *United States v. Montieth*, 662 F.3d 660, 664 (4th Cir. 2011). In determining whether probable cause exists, the issuing judge is confined to the averments contained in the four corners of the search warrant application. *See United States v. Hurwitz*, 459 F.3d 463, 470-71 (4th Cir. 2006).

The concept of probable cause "defies a precise definition[.]" *United States v. Richardson*, 607 F.3d 357, 369 (4th Cir. 2010). Indeed, it is a flexible standard and a "fluid concept," *Maryland v. Pringle*, 540 U.S. 366, 370 (2003), which is not "readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 232; *see United States v. Ventresca*, 380 U.S. 102, 108 (1965); *United States v. Drummond*, 925 F.3d 681, 687 (4th Cir. 2019); *United States v. Allen*, 631 F.3d 164, 172 (4th Cir. 2011).

The Court said in *Gates*, 462 U.S. at 238:

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.

Accord *Pringle*, 540 U.S. at 370 (reiterating that probable cause is a "'practical, nontechnical conception' that deals with the 'factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act'") (cleaned up). Notably, the standard is "not a high bar." *Kaley v. United States*, 571 U.S. 320, 338 (2014).

The probable cause analysis is based on the totality of the circumstances, rather than a "'technical dissection'" of the circumstances. *District of Columbia v. Wesby*, ___ U.S. ___, 138 S. Ct. 577, 588 (2018) (citation omitted); *see Gates*, 462 U.S. at 238. Thus, the issuing court does not consider each fact "'in isolation' . . . ." *Wesby*, 138 S. Ct. at 588; *see Drummond*, 925 F.3d at 687. "The totality-of-the-circumstances test 'precludes this sort of divide-and-conquer analysis.'" *Wesby*, 138 S. Ct. at 588 (quoting *United States v. Arvizu*, 534 U.S. 266, 274 (2002)). In other words, "'the whole picture'" must be considered, because "the whole is often greater than the sum of its parts . . . ." *Wesby*, 138 S. Ct. at 588 (citation omitted); *accord Drummond*, 925 F.3d at 687.

To be sure, there are "limits beyond which a magistrate may not venture in issuing a warrant," *Gates*, 462 U.S. at 239, and "[d]eference to the magistrate . . . is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984); *see Smith v. Munday*, 848 F.3d 248, 255 (4th Cir. 2017). Even a generous, non-technical review of a warrant cannot be used to scuttle the protections of the Fourth Amendment. To the contrary, "[s]ufficient information must be presented to the magistrate to allow that official to determine probable cause; his actions cannot be a mere ratification of the bare conclusions of others." *Gates*, 462 U.S. at 239. Thus, "the Government cannot rely upon post hoc rationalizations to validate those seizures that happen to turn up contraband." *United States v. Foster*, 634 F.3d 243, 249 (4th Cir. 2011).

Moreover, an affidavit must establish probable cause for the belief that the suspect occupies or is otherwise connected to the targeted premises or that contraband or evidence will be found in that particular place. *United States v. Grubbs*, 547 U.S. 90, 97 (2006); *United States v. Cobb*, 970 F.3d 319, 326 (4th Cir. 2020); *see Gates*, 462 U.S. at 238; *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013); *Davis*, 690 F.3d at 241. As the Fourth Circuit explained in

*Cobb*, 970 F.3d at 326, the Fourth Amendment "'specifies only two matters that must be 'particularly described' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'" (Quoting *Grubbs*, 547 U.S. at 97) (alteration omitted); *see also United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020). And, "'[t]here is a practical margin of flexibility permitted by the constitutional requirement for particularity in the description of items to be seized.'" *Cobb*, 970 F.3d at 326 (citation omitted).

So, to be valid, a warrant affidavit must establish a sufficient nexus between the place to be searched and the criminal activity. *United States v. Allen*, 631 F.3d 164, 173 (4th Cir. 2011). This requires a "fair probability" that evidence of the crime will be found at the place to be searched. *Gates*, 462 U.S. at 238. But, the Fourth Circuit "long [has] held that an affidavit need not directly link the evidence sought with the place to be searched." *United States v. Jones*, 942 F.3d 534, 639 (2019). Rather, and of relevance here, "'the nexus between the place to be searched and the items to be seized may be established by the nature of the item and the normal inferences of where one would likely keep such evidence.'" *United States v. Doyle*, 650 F.3d 460, 471 (4th Cir. 2011) (citation omitted); *see also United States v. Anderson*, 851 F.2d 727, 729 (4th Cir. 1988).

Thus, nexus may be established even when the affidavit in support of the search warrant does not contain facts establishing a direct link to the items sought in the residence. *United States v. Grossman*, 400 F.3d 212, 217 (4th Cir. 2005); *see also United States v. Williams*, 548 F.3d 311, *United States v. Servance*, 394 F.3d 222, 230 (4th Cir. 2005), *vacated on other grounds*, 544 U.S. 1047 (2005); *United States v. Moore*, 477 Fed. App'x. 102, 105 (4th Cir. 2012); *United States v. Williams*, 974 F.2d 480 (4th Cir. 1992). Moreover, law enforcement officers "may draw conclusions from their experience, judgment, and observations when

identifying the place to be searched." *United States v. Wienke*, 733 Fed. App'x 65, 69-70 (4th Cir. 2018); *see also United States v. Ortiz,* 422 U.S. 891, 897 (1975) (stating that "officers are entitled to draw reasonable inferences from the[] facts in light of their knowledge of the area and their prior experience. . . ."); *United States v. Brignoni-Ponce,* 422 U.S. 873, 885 (1975) (concluding that "the officer is entitled to assess the facts in light of his experience. . . ."); *United States v. Moore*, 477 Fed. Appx 102 (4th Cir. 2012).

Here, the affiant, TFC Donald, described his training in internet usage as it pertains to sexual offenses involving children. *See, e.g.*, ECF 44-8 at 2; Gov't Ex. 8 at 5. Further, based on his training, the affiant averred that computers are used in such crimes, including hard drives and laptops, and he claimed that such materials are often stored for lengthy periods. *Id.* at 4-5.

Moreover, the affiant recounted information provided by defendant's co-worker. Although the co-worker's name was not disclosed, his identity was known; the co-worker submitted to a recorded interview with the affiant. *Id.* at 10. Notably, the co-worker reported that he saw a disturbing image of a child on defendant's work computer. *Id.* at 11. Further, he claimed that the defendant "always takes his personal laptop with him to and from work." *Id.* In addition, the co-worker told the affiant that every night the defendant takes home a computer back-up drive. *Id.* at 12.

Further, by that point the affiant knew of the child pornography found on the defendant's work computer. *Id.* at 12. And, the work computer had cables attached to it for use with another external hard drive, but that hard drive was not evident during the first search in March 2019. *Id.* In addition, the affiant was aware of defendant's prior sex offense conviction. *Id.* at 11-12.

Applying commonsense and considering the totality of the circumstances, the affidavit established a nexus to defendant's home, sufficient to give rise to probable cause.

**D. Good Cause**

Even assuming, *arguendo*, that one or more warrant applications were deficient, the exclusionary rule would not apply here.

When a search violates the Fourth Amendment, "evidence obtained in violation of the Fourth Amendment" may be inadmissible under the exclusionary rule, which is "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect. . . ." *United States v. Calandra*, 414 U.S. 338, 348 (1974); *see United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017); *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014). The exclusionary rule "serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *United States v. McLamb*, 880 F.3d 685, 690 (4th Cir. 2018). It has as its purpose the deterrence of "future" Fourth Amendment violations. *Davis v. United States*, 564 U.S. 229, 236-37 (2011).

However, exclusion exacts a "heavy toll" on "the judicial system and society at large." *Davis*, 564 U.S. at 237. Indeed, the Supreme Court has characterized exclusion as a "harsh sanction," *id*. at 241, and "the last resort . . . ." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Notably, deterrence "is not achieved through the suppression of evidence obtained by 'an officer acting with objective good faith'" pursuant to a search warrant issued by a judicial officer. *United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004) (citation omitted); *see Stephens*, 764 F.3d at 335.

In *United States v. Leon*, 468 U.S. 897 (1984), and the companion case of *Massachusetts v. Sheppard*, 468 U.S. 981 (1984), the Supreme Court recognized a good faith exception to the exclusionary rule. Notwithstanding the importance of the exclusionary rule to Fourth Amendment jurisprudence, the *Leon* Court determined that "suppression of evidence obtained

pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Leon*, 468 U.S. at 918. The Court reasoned, *id.* at 922: "We conclude that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."

Thus, *Leon* provides for the admissibility of evidence seized pursuant to a warrant subsequently determined to be invalid, if the "officers acted in the objectively reasonable belief that their conduct did not violate the Fourth Amendment." *Id.* In *Sheppard*, 468 U.S. at 989-90, the Supreme Court added: "[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him . . . that the warrant he possesses authorizes him to conduct the search he has requested." Thus, ordinarily, a "'warrant issued by a magistrate . . . suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" *Leon*, 468 U.S. at 922 (citation omitted).

The cases are legion in this regard. *See, e.g.*, *Herring v. United States*, 555 U.S. 135, 145 (2009); *United States v. Fall*, 955 F.3d 363, 371 (4th Cir. 2020); *Lyles*, 910 F.3d at 796; *United States v. Thomas*, 908 F.3d 68, 73 (4th Cir. 2018); *United States v. Chavez*, 894 F.3d 593, 608 (4th Cir. 2018); *Doyle*, 650 F.3d at 467; *United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004).

The *Leon* standard is an objective one. *Thomas*, 908 F.3d at 70. *Leon* teaches that the "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal" in light of "all of the circumstances." 468 U.S. at 922 n.23; *see also Stephens*, 764 F.3d at 335; *United States v. McKenzie-Gude*, 671 F.3d 452, 459 (4th Cir. 2011). Thus, "the officer's reliance on the

magistrate's probable-cause determination . . . must be objectively reasonable, and it is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 922-23 (citations and footnotes omitted). In other words, suppression is not appropriate when "the police act with an objectively reasonable good-faith belief that their conduct is lawful." *United States v. Rush*, 808 F.3d 1007, 1010 (4th Cir. 2015).

Under *Leon*, 468 U.S. at 922, there are four circumstances when exclusion of evidence remains the appropriate sanction, even if an officer "has obtained a warrant and abided by its terms." The four situations when the sanction of exclusion is an appropriate remedy are as follows: 1) if the magistrate or judge who issued the warrant was misled by information in an affidavit that the affiant knew was false or would have known but for his reckless disregard for the truth; 2) if the issuing magistrate wholly abandoned his judicial role; 3) the affidavit supporting the warrant is "'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'"; 4) the warrant is "so facially deficient — i.e., in failing to particularize the place to be searched or the things to be seized — that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923 (citations omitted). *See United States v. Wellman*, 663 F.3d 224, 228-29 (4th Cir. 2011); *United States v. DeQuasie*, 373 F.3d 509, 519-520 (4th Cir. 2004).

The *Leon* Court said, 468 U.S. at 926:

> In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.

In this case, none of the four circumstances outlined above has been established. Even assuming, *arguendo*, that a search warrant application was deficient, the good faith standard would apply.

**III. Conclusion**

For the reasons set forth above, I shall deny the Motion.

An Order follows.

Date: May 28, 2021

/s/
Ellen L. Hollander
United States District Judge